PATENT APPLICATION
DOCKET NO. 100201141-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

INVENTOR(S): Gregory Eugene Perkins, et al.

SERIAL NO.: 10/085,927 **GROUP ART UNIT:** 2141

FILED: Feb. 27, 2002 **EXAMINER:** Bayard, Djenane M

SUBJECT: RESOURCE LOCATION AND ACCESS

APPELLANTS'/APPLICANTS' THIRD OPENING BRIEF ON APPEAL

1. REAL PARTY IN INTEREST.

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holding, LLC.

2. RELATED APPEALS AND INTERFERENCES.

There are no other appeals or interferences known to Appellants, Appellants' legal representative or the Assignee which will affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS.

Claims 1-25 are pending. Claims 1-7, 9-15, and 17-25 stand rejected. Claims 8 and 16 have been deemed allowable but stand rejected to as being dependent from a rejected base claim. All pending rejected claims are appealed.

4. STATUS OF AMENDMENTS.

No amendments to the Specification or Claims have been filed after the latest action was entered.

5. SUMMARY OF CLAIMED SUBJECT MATTER.

Claim 1 recites a method for locating a resource in a computer network that includes providing an interface having instructions to send association data. *See, e.g.*, Specification, paragraph [0038]. An identity service is identified using the association data. *See, e.g.*, Specification, paragraphs [0040] and [0041]. The identity service manages resource data. *See, e.g.*, Specification, paragraphs [0040] and [0041]. The resource is located using the resource data. *See, e.g.*, Specification, paragraph [0043].

Claim 5 recites a method for locating a resource for a user in a computer network where that method includes providing an interface having instructions to send association data to two or more association services. *See, e.g.*, Specification, paragraph [0038]. From the two or more association services, an association service with which the user has established a relationship is identified. *See, e.g.*, Specification, paragraph [0040]. Using the association data sent to the identified association service, an identity service is identified. *See, e.g.*, Specification, paragraphs [0040] and [0041]. The identity service manages resource data. *See, e.g.*, Specification, paragraphs [0040] and [0041]. The resource is located using the resource data. *See, e.g.*, Specification, paragraph [0043].

Claim 6 recites a method for locating a resource in a computer network that includes providing a web page having instructions to request a web bug. *See, e.g.*, Specification, paragraph [0036]. The web bug is requested by sending a cookie and an URL for the web page. *See, e.g.*, Specification, paragraph [0036]. The cookie and the URL are saved for the web page as an entry in an association table. *See, e.g.*, Specification, paragraph [0036]. Providing the URL for the web page, the association table is queried for the cookie in the entry containing the URL. *See, e.g.*, Specification, paragraphs [0040] and [0041]. Other entries in the association table containing the cookie are identified. *See, e.g.*, Specification, paragraphs [0040] and [0041]. From those entries an entry containing an URL for an identification service is identified. *See, e.g.*, Specification, paragraphs [0040] and [0041]. The identification service manages resource data. *See, e.g.*, Specification, paragraphs [0040] and [0041]. The resource is located using the resource data. *See, e.g.*, Specification, paragraph [0043].

Claim 7 recites a method for producing an electronic document where that method includes generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options. *See, e.g.*, Specification, paragraphs [0045]-[0049]. Providing an URL for the generated web page, the association service is

queried to identify an identity service with which the user is registered. *See, e.g.*, Specification, paragraphs [0045]-[0049]. The user's resource data is obtained from the identified identity service. *See, e.g.*, Specification, paragraphs [0045]-[0049]. A document management service is located and accessed using the resource data. *See, e.g.*, Specification, paragraphs [0045]-[0049]. Additional content for the web page is provided for displaying controls for selecting a document managed by the document management service. *See, e.g.*, Specification, paragraphs [0045]-[0049]. A document is produced according to selections made through the web page. *See, e.g.*, Specification, paragraphs [0045]-[0049].

Claim 9 recites a computer readable medium having instructions for implementing various acts. Those acts include (1) providing an interface having instructions to send association data; (2) identifying an identity service using the association data, the identity service managing resource data; and (3) locating a resource using the resource data. *See, e.g.*, Specification, paragraphs [0038]-[0043].

Claim 13 recites a computer readable medium having instructions for performing various acts. Those acts include (1) providing an interface having instructions to send association data to two or more association services; (2) identifying from the two or more association services, an association service with which a user has established a relationship; (3) identifying an identity service using the association data sent to the identified association service, the identity service managing resource data; and (4) locating a resource for the user using the resource data. *See, e.g.*, Specification, paragraphs [0038]-[0043].

Claim 14 recites a computer readable medium having instructions for performing various acts. Those acts include (1) providing a web page having instructions to request a web bug; (2) requesting the web bug sending a cookie and an URL for the web page; (3) saving the cookie and the URL for the web page as an entry in an association table; (4) querying, providing the URL for the web page, the association

table for the cookie in the entry containing the URL; (5) identifying another entries in the association table containing the cookie; (6) identifying, from those entries, the entry containing an URL for an identification service, the identification service managing resource data; and (7) locating a resource using the resource data. *See, e.g.*, Specification, paragraphs [0036]-[0043].

Claim 15 recites a computer readable medium having instructions for performing various tasks. Those tasks include generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options and querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page. *See, e.g.*, Specification, paragraphs [0045]-[0049]. The tasks include obtaining the user's resource data from the identified identity service and locating and accessing a document management service using the resource data. *See, e.g.*, Specification, paragraphs [0045]-[0049]. The tasks also include providing additional content for the web page for displaying controls for selecting a document managed by the document management service and producing a document according to selections made through the web page. *See, e.g.*, Specification, paragraphs [0045]-[0049].

Claim 17 recites a system for locating a resource that includes an association module and an application. *See, e.g.*, Specification, paragraph [0024]. The association module is operable to query an association service, supplying a session identifier, in order to identify an identity service managing resource data. *See, e.g.*, Specification, paragraphs [0024]-[0026], [0027], and [0040]. The application is operable to (1) provide an interface having instructions to send association data to the association service, the association data to contain a client identifier and a session identifier for the provided interface; (2) acquire resource data from an identity service identified by a query from the association module; and (3) locate the resource using the resource data. *See, e.g.*, Specification, paragraphs [0038]-[0043].

Claim 19 recites a document production system that includes an association module and a document production application. *See, e.g.*, Specification, paragraph [0024]. The association module is operable to query an association service, supplying a session identifier in order to identify an identity service managing resource data. *See, e.g.*, Specification, paragraphs [0024]-[0026], [0027], and [0040]. The document production application is operable to perform various tasks. Those tasks include providing an interface having content for sending association data containing a session identifier for the provided interface to an association service as well as content for displaying controls for selecting production options. *See, e.g.*, Specification, paragraphs [0045]-[0049]. The tasks include acquiring resource data from an identity service identifier identified by a query from the association module and locating and accessing a document management service using the resource data. *See, e.g.*, Specification, paragraphs [0045]-[0049]. The tasks also include providing, for the interface, additional content for displaying controls for selecting a document managed by the document management service and producing a document according to selections made through the interface. *See, e.g.*, Specification, paragraphs [0045]-[0049].

Claim 20 recites a system for locating a resource where that system includes an identity service, an association server, an association table interface, an association module, and an application. *See, e.g.*, Specification, paragraphs [0024]-[0028]. The identity service is operable to manage resource data. *See, e.g.*, Specification, paragraphs [0022] and [0026]. The association server is operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table. *See, e.g.*, Specification, paragraph [0027]. The association table interface is in communication with the association server and is operable, according to a received query, to access from the association table a session identifier for the identity service using a session identifier supplied with the query. *See, e.g.*, Specification, paragraph

[0027]. The association module is operable to query, supplying a session identifier, the association service in order to identify the identity service. *See, e.g.*, Specification, paragraph [0040]. The application is operable to (1) provide an interface having instructions to send association data to an association server, the association data to contain a client identifier and a session identifier for the provided interface; (2) acquire resource data from the identity service identified by a query from the association module; and (3) locate the resource using the resource data. *See, e.g.*, Specification, paragraphs [0038]-[0043].

Claim 22 recites a document production system that includes a document management service, an identity service, an association server, an association table interface, an association module, and a document production application. *See, e.g.*, Specification, paragraphs [0024]-[0028] and [0044]. The identity service is operable to manage resource data for locating and accessing the document management service. *See, e.g.*, Specification, paragraphs [0022] and [0026]. The association server is operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table. *See, e.g.*, Specification, paragraph [0027]. The association table interface is in communication with the association server and is operable, according to a received query, to access from the association table a session identifier for the identity service using the session identifier supplied with the query. *See, e.g.*, Specification, paragraph [0027]. The association module operable to query, supplying a session identifier, the association service in order to identify the identity service. *See, e.g.*, Specification, paragraph [0040]. The a document production application operable to perform various tasks. Those tasks include providing an interface having content for sending association data containing a client identifier and a session identifier for the provided interface to an association service as well as content for displaying controls for selecting production options. The tasks include acquiring resource data from an identity service using the session identifier for the identity service identified by a query from the association module and locating and access the document management service using

the resource data. The tasks also include providing, for the interface, additional content for displaying controls for selecting a document managed by the document management service and producing a document according to selections made through the interface. *See, e.g.*, Specification, paragraphs [0045]-[0049].

Claim 24 recites a system for locating a resource. That system includes a means for querying, supplying a session identifier, an association service in order to identify an identity service managing resource data. The system includes a means for providing an interface having instructions to send association data to the association service, the association data to contain a client identifier and a session identifier for the provided interface. The system also includes a means for acquiring resource data from an identity service identified by a query and a means for locating the resource using the resource data. *See, e.g.*, Specification, paragraphs [0024]-[0028] and [0038]-[0043].

Claim 25 recites a document production system that includes a means for querying, supplying a session identifier, an association service in order to identify an identity service managing resource data. The system includes a means for providing an interface having content for sending association data containing a session identifier for the provided interface to the association service as well as content for displaying controls for selecting production options. The system includes a means for acquiring resource data from an identity service identifier identified by a query. The system includes a means for locating and accessing a document management service using the resource data. The system also includes a means for providing, for the interface, additional content for displaying controls for selecting a document managed by the document management service and a means for producing a document according to selections made through the interface. *See, e.g.*, Specification, paragraphs [0024]-[0028] and paragraphs [0045]-[0049].

6. GROUNDS FOR REJECTION TO BE REVIEWED.

A. Claims 9 and 13-15 stand rejected under 35 USC §101 as being directed

to non-statutory subject matter.

B. Claims 1, 2, 5, 9-10, 13, 17-25 stand rejected under 35 USC §102 as being anticipated by USPN 6,490,624 issued to Sampson.

C. Claims 3 and 11stand rejected under 35 USC §103 as being unpatentable over Sampson in view of US Pub 2003/0074580 to Knouse.

D. Claims 4 and 12 stand rejected under 35 USC §103 as being unpatentable over Sampson in view of Knouse and in further view of USPN 2004/0015580 to Lu.

E. Claims 6 and 14 stand rejected under 35 USC §103 as being unpatentable over Knouse and in further view of Lu.

F. Claims 7 and 15 stand rejected under 35 USC §103 as being unpatentable over Sampson in further view of Lu.

7. ARGUMENT.

Grounds For Rejection A – Claims 9 and 13-15 stand rejected under 35 USC §101 as being directed to non-statutory subject matter.

MPEP 2106.01(I) indicates that a computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized **IS** statutory. The preamble of each of Claims 9, and 13-15 recites a computer readable medium having instructions for performing various tasks. One can infer from such a preamble, that the computer can read the recited instructions and be caused to perform the recited tasks. As such, Claim 9 and Claims 13-15 each define structural and functional interrelationships

between the computer program and the rest of the computer which permit the computer program's functionality to be realized and are statutory.

Furthermore, MPEP 2106 sets out guidelines for patent subject matter eligibility. Generally speaking the Unite States Supreme Court has ruled that "anything under the sun that is made by man" is statutory subject matter under §101. MPEP 2106(IV)(A). However, there are judicial exceptions. These include laws of nature, natural phenomena, and abstract ideas. MPEP 2106(IV)(C). The MPEP also states that a practical application of one of the judicial exemptions can qualify for patent protection. MPEP 2106(IV)(C)(1). In other words a claim that includes excluded subject matter is patentable if that claim is for a practical application of the abstract idea, law of nature, or natural phenomena. MPEP 2106(IV)(C)(2).

The MPEP sets out a test for determining if a claimed invention is directed to a practical application of one of the judicial exception. A claim is patentable under §101 when it:

(A) "transforms" an article or physical object to a different state or thing; or

(B) otherwise produces a useful, concrete and tangible result, based on the factors discussed below.

MPEP 2106(IV)(C)(2). In making a determination as to whether the claimed invention produces a useful, concrete and tangible result, the focus is not on whether the steps taken to achieve a particular result are useful, concrete and tangible. Instead, the focus is on whether the final result achieved by the claimed invention is useful, concrete and tangible. MPEP 2106(IV)(C)(2).

Useful: For an invention to be useful, the utility need be specific, substantial, and credible. MPEP 2106(IV)(C)(2)(a) (relying on MPEP 2607). .When an applicant asserts that the claimed invention is useful for any particular practical purpose and the assertion would be considered credible by a person of ordinary skill in the art, the Examiner may not impose a rejection based on lack of utility. MPEP 2107(B)(1)

Credibility of the assertion is determined in view of the applicant's disclosure. MPEP 2107(B)(1)(ii).

Tangible: To be tangible a claim need not be tied to a particular machine or apparatus – the claim need only recite more than just a judicial exception. That is, to be tangible a claim need recite more than just a law of nature, a natural Phenomena, and/or and abstract idea. MPEP 2106(IV) (C)(2)(b). The MPEP specifically states that the opposite meaning of "tangible" is abstract. MPEP 2106(IV) (C)(2)(b).

Concrete: A claim produces a concrete result where that result is repeatable. In other words a claimed process is concrete if the result can be substantially repeatable. MPEP 2106(IV) (C)(2)(c). The MPEP specifically states that the opposite meaning of "concrete"" is unrepeatable or unpredictable. MPEP 2106(IV) (C)(2)(c).

Claim 9 is directed to a computer readable medium having instructions for:

1. providing an interface having instructions to send association data;
2. identifying an identity service using the association data, the identity service managing resource data; and
3. locating a resource using the resource data.

The result of the computer's execution of the recited instructions is the location of a particular resource using resource data managed by an identity service that was identified using association data. The association data is sent or otherwise obtained as a result of the provision of a user interface that has instructions to send the association data. As such Claim 9 recites a computer-readable medium encoded with a computer program which defines, at least implicitly, the structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized. Furthermore, Claim 9 is useful and tangible. Those instructions can be executed repeatedly so the process is repeatable and therefore Claim 9 is concrete.

Claim 13 is directed to a computer readable medium having instructions for:

1. providing an interface having instructions to send association data to two or more association services;
2. identifying from the two or more association services, an association service with which a user has established a relationship;
3. identifying an identity service using the association data sent to the identified association service, the identity service managing resource data; and
4. locating a resource for the user using the resource data.

Like Claim 9, the result of the computer's execution of the recited instructions is the location of a particular resource using resource data managed by an identity service that was identified using association data. However, in Claim 13, the particular one of two association services is also identified. The association data is sent or otherwise obtained as a result of the provision of a user interface that has instructions to send association data to the two association services. As such Claim 13 recites a computer-readable medium encoded with a computer program which defines, at least implicitly, the structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized. Furthermore, Claim 13 is useful and tangible. Those instructions can be executed repeatedly so the process is repeatable and therefore Claim 13 is concrete.

Claim 14 is directed to a computer readable medium having instructions for:

1. providing a web page having instructions to request a web bug;
2. requesting the web bug sending a cookie and an URL for the web page;
3. saving the cookie and the URL for the web page as an entry in an association table;

4. querying, providing the URL for the web page, the association table for the cookie in the entry containing the URL;
5. identifying another entries in the association table containing the cookie;
6. identifying, from those entries, the entry containing an URL for an identification service, the identification service managing resource data; and
7. locating a resource using the resource data.

Like Claims 9 and 13, the result of the computer's execution of the recited instructions is the location of a particular resource using resource data managed by an identity service that was identified using association data. However, in Claim 14, the association data takes the form of a cookie containing an URL of the identity service that manages the resource data. As such Claim 14 recites a computer-readable medium encoded with a computer program which defines, at least implicitly, the structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized. Furthermore, Claim 14 is useful and tangible. Those instructions can be executed repeatedly so the process is repeatable and therefore Claim 14 is concrete.

Claim 15 is directed to a computer readable medium having instructions for:

1. generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options;
2. querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page;
3. obtaining the user's resource data from the identified identity service;
4. locating and accessing a document management service using the resource data;
5. providing additional content for the web page for displaying controls for

selecting a document managed by the document management service; and

6. producing a document according to selections made through the web page.

The result of the computer's execution of the recited instructions is the production of a document according to selections made through a web page. The particular document produced is managed by a recourse labeled as a document management service. The document management service is located and accessed using resource data obtained from an identity service. As such Claim 15 recites a computer-readable medium encoded with a computer program which defines, at least implicitly, the structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized. Furthermore, Claim 15 is useful and tangible. Those instructions can be executed repeatedly so the process is repeatable and therefore Claim 15 is concrete.

For at least these Reasons, Claims 9 and 13-15 have practical application and are directed to statutory subject matter under §101.

Grounds For Rejection B – Claims 1, 2, 5, 9-10, 13, 17-18, and 20-25 stand rejected under 35 USC §102 as being anticipated by USPN 6,490,624 issued to Sampson.

The Appellants are concerned by the Examiner's reliance on Sampson. The Examiner cited Sampson as the basis for a §102 rejection of many of the same claims in an office actions mailed October 19, 2005 and April 6, 2006. On June The Appellants filed a notice of appeal and supporting brief addressing those §102 rejections. In response, the Examiner reopened prosecution on October 18, 2006 stating that the "Applicant's arguments, presented in appeal brief with respect to the rejection(s) of claim(s) 1-25 have been fully considered and are persuasive."

However, the Examiner cited new grounds for rejection. The Appellants responded filing a second notice of appeal and second opening brief on May 18, 2007. The Examiner has again reopened prosecution and is, without explanation, once again relying on Sampson to support a §102 rejection even though the Examiner has previously agreed that the same Claims were patentable over Sampson. The Examiner's inconsistent positions leaves the Appellant in a difficult position.

Sampson is directed to session management in a stateless network such as the Internet. *See, e.g.,* Sampson, Title and Abstract. Sampson's system includes a number of access servers each of which acts as a gatekeeper for a protected server. Session information for a given client is stored in a session manager bound to an access server. In operation a client logs into an access server for a first protected server and then submits a request for a resource of a second protected server. The session manger for the access server determines whether the client has any authenticated sessions with any other access servers. If so, the client is permitted to access the resource of the second protected server without first logging in. *See* Sampson, Abstract.

Claim 1 is directed to a method for locating a resource and recites the following acts:

1. providing an interface having instructions to send association data;
2. identifying an identity service using the association data, the identity service managing resource data; and
3. locating the resource using the resource data.

Citing Sampson, the Examiner, at page 3 of the latest office action contends that each act of Claim 1 is taught by Sampson, col. 7, line 64 through Col. 8, line 5. In addition, the Examiner makes a cryptic reference to "Protected web server." The cited passage is reproduced below:

> When the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server. A Protected Web Server is a web server with resources protected by the Runtime Module. The Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource. The cookie is also used by the resource to return information that is customized based on the user's name and roles.

Sampson, col. 7, line 64 through col. 8, line 4. While not clear, it appears that the Examiner equates (a) Sampson's cookie with the recited association data and (b) Sampson's Protected web server with the recited identity service. The Examiner's position is confused at best.

Sampson teaches that the cookie (association data?) is used by a runtime module to verify that the user is authorized to access the resource and used by the resource to return information that is customized based on the user's name and roles. Sampson mentions nothing of using the Cookie to identify an identity service that manages resource data. Further the passage mentions nothing of identifying a resource using that resource data.

In the first opening brief filed June 27, 2006, the Appellant explained that Sampson describes a system in which a client makes a request for a document from a protected server. Sampson, col. 12, lines 65-67. As a consequence, a runtime sends a message to a session object requesting validation of a session between the client and the protected server. Sampson, col. 13, lines 1-3. The message includes a "Session ID." Sampson, col. 13, lines 4-5. A cookie is an example of a session ID.

Sampson's session manager takes the Session ID and performs a series of tasks that include:

(1) ensuring that the Session ID is in a hash table (col. 13, lines 6-18);

(2) determining whether the Session ID has been revoked (col. 13, lines 19-23);

(3) determining whether an idle time out has occurred with respect to the Session ID (col. 13, lines 24-28); and

(4) generating a status code for the Status ID (col. 13, lines 29-39);

Sampson's runtime then performs tasks that include:

(1) allowing the client access to the protected server according to the status code (col. 13, lines 34-39);
(2) denying the client access to the protected server and sending the client a message explaining why (col. 13, lines 40-53).

Sampson's Session ID or cookie is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Consequently, Sampson fails to teach a method that includes identifying an identity service using the association data, the identity service managing resource data. For at least this reason, Claim 1 is patentable over Sampson. Claims 2-4 are also patentable over Sampson due at least in part to their dependence from Claim 1.

Claim 5 is directed to a method for locating a resource for a user and recites the following acts:

1. providing an interface having instructions to send association data to two or more association services;
2. identifying from the two or more association services, an association service with which the user has established a relationship;
3. identifying an identity service using the association data sent to the identified association service, the identity service managing resource data; and
4. locating the resource using the resource data.

As for the act of identifying an identity service using the association data, the Examiner once cites Sampson, col. 13, lines 6-17. The cited passage is taken from a

subsection of Sampson entitled "Run Time Operation of Session Managers." Sampson, col. 10, line 62. In that subsection Sampson describes a system in which a client makes a request for a document from a protected server. Sampson, col. 12, lines 65-67. As a consequence, a runtime sends a message to a session object requesting validation of a session between the client and the protected server. Sampson, col. 13, lines 1-3. The message includes a "Session ID." Sampson, col. 13, lines 4-5.

Sampson's session manager takes the Session ID and performs a series of tasks that include:

(1) ensuring that the Session ID is in a hash table (col. 13, lines 6-18);
(2) determining whether the Session ID has been revoked (col. 13, lines 19-23);
(3) determining whether an idle time out has occurred with respect to the Session ID (col. 13, lines 24-28); and
(4) generating a status code for the Status ID (col. 13, lines 29-39);

Sampson's runtime then performs tasks that include:

(1) allowing the client access to the protected server according to the status code (col. 13, lines 34-39);
(2) denying the client access to the protected server and sending the client a message explaining why (col. 13, lines 40-53).

A review of the passage relied on by the Examiner reveals that Sampson's Session ID is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Consequently, Sampson fails to teach a method that includes identifying an identity service using the association data, the identity service managing resource data. For at least this reason, Claim 5 is patentable over Sampson.

Claim 9 is directed to a computer readable medium having instructions for implementing the method of Claim 1. For at least the same reasons Claim 1 is patentable, so are Claim 9 and Claims 10-12 which depend from Claim 9.

Claim 13 is directed to a computer readable medium having instructions for implementing the method of Claim 5. For at least the same reasons Claim 5 is patentable, so is Claim 13.

Claim 17 is direct to a system for locating a resource, and recites the following elements:

1. an association module operable to query an association service, supplying a session identifier, in order to identify an identity service managing resource data; and
2. an application operable to:
    a. provide an interface having instructions to send association data to the association service, the association data to contain a client identifier and a session identifier for the provided interface;
    b. acquire resource data from an identity service identified by a query from the association module; and
    c. locate the resource using the resource data.

In short, Claim 17 recites a system capable of implementing the method of Claim 1. For at least the same reasons Claim 1 is patentable, so is Claim 17 and Claim 18 which depends from Claim 17.

Claim 19 is directed to a document production system and recites the following elements:

1. an association module operable to query an association service, supplying a session identifier in order to identify an identity service managing resource data; and
2. a document production application operable to:
    a. provide an interface having content for sending association data containing a session identifier for the provided interface to an association service as well as content for displaying controls for selecting production options;
    b. acquire resource data from an identity service identifier identified by a query from the association module;
    c. locate and access a document management service using the resource data; and
    d. provide, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and
    e. produce a document according to selections made through the interface.

The Examiner asserts that the association module element of Claim 19 is taught by Sampson, col. 13, lines 1-17. As discussed above with respect to Claim 5, the cited passage explains that Sampson's session manager takes the Session ID and performs a series of tasks that include ensuring that the Session ID is in a hash table. Sampson, col. 13, lines 6-18. Sampson's Session ID is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Nothing in Sampson teaches an association module as that element is recited in Claim 19. More particularly Sampson fails to teach or suggest "an association module operable to query an association service, supplying a session identifier in order to

identify an identity service managing resource data." For at least this reason, Claim 19 is patentable over Sampson.

Claim 20 is directed to a system for locating a resource and recites the following elements:

1. an identity service operable to manage resource data;
2. an association server operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table;
3. an association table interface in communication with the association server and operable, according to a received query, to access from the association table a session identifier for the identity service using a session identifier supplied with the query;
4. an association module operable to query, supplying a session identifier, the association service in order to identify the identity service;
5. an application operable to:
    a) provide an interface having instructions to send association data to an association server, the association data to contain a client identifier and a session identifier for the provided interface;
    b) acquire resource data from the identity service identified by a query from the association module; and
    c) locate the resource using the resource data.

The Examiner asserts that the association module element of Claim 20 is taught by Sampson, col. 13, lines 6-13 stating "*the session manager object checks to determine whether the session Id is recognized or known.*"

As discussed above with respect to Claim 5, the cited passage explains that Sampson's session manager takes the Session ID and performs a series of tasks that include ensuring that the Session ID is in a hash table. Sampson, col. 13, lines 6-18.

Sampson's Session ID is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Nothing in Sampson teaches an association module as that element is recited in Claim 20. More particularly Sampson fails to teach or suggest an "association module operable to query, supplying a session identifier, the association service in order to identify the identity service." For at least this reason, Claim 20 is patentable over the cited references as is Claim 21 which depends from Claim 20.

Claim 22 is directed to a document production system and recites the following elements:

1. a document management service;
2. an identity service operable to manage resource data for locating and accessing the document management service;
3. an association server operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table;
4. an association table interface in communication with the association server and operable, according to a received query, to access from the association table a session identifier for the identity service using the session identifier supplied with the query;
5. an association module operable to query, supplying a session identifier, the association service in order to identify the identity service;
6. a document production application operable to:
    a. provide an interface having content for sending association data containing a client identifier and a session identifier for the provided

interface to an association service as well as content for displaying controls for selecting production options;

b. acquire resource data from an identity service using the session identifier for the identity service identified by a query from the association module;
c. locate and access the document management service using the resource data;
d. provide, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and
e. produce a document according to selections made through the interface.

The Examiner asserts that the association module element of Claim 20 is taught by Sampson, col. 13, lines 1-17. As discussed above with respect to Claim 5, the cited passage explains that Sampson's session manager takes the Session ID and performs a series of tasks that include ensuring that the Session ID is in a hash table. Sampson, col. 13, lines 6-18. Sampson's Session ID is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Nothing in Sampson teaches an association module as that element is recited in Claim 20. More particularly Sampson fails to teach or suggest an "association module operable to query, supplying a session identifier, the association service in order to identify the identity service." For at least this reason, Claim 22 is patentable over Sampson as is Claim 23 which depends from Claim 22.

Claim 24 is directed to a system for implementing the method of Claim 1. For at least the same reasons Claim 1 is patentable, so is Claim 24.

Claim 25 is directed to a document production system that includes the following:

a. a means for querying, supplying a session identifier, an association service in order to identify an identity service managing resource data;
b. a means for providing an interface having content for sending association data containing a session identifier for the provided interface to the association service as well as content for displaying controls for selecting production options;
c. a means for acquiring resource data from an identity service identifier identified by a query;
d. a means for locating and accessing a document management service using the resource data;
e. a means for providing, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and
f. a means for producing a document according to selections made through the interface.

The Examiner asserts that the means for querying is taught by Sampson, col. 13, lines 1-17. As discussed above with respect to Claim 5, the cited passage explains that Sampson's session manager takes the Session ID and performs a series of tasks that include ensuring that the Session ID is in a hash table. Sampson, col. 13, lines 6-18. Sampson's Session ID is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Nothing in Sampson teaches a means for querying as that element is recited in Claim 20. More particularly Sampson fails to teach or suggest "a means for querying, supplying a session identifier, an association service in order to identify an identity

service managing resource data." For at least this reason, Claim 25 is patentable over Sampson.

Grounds For Rejection C – Claims 3 and 11 stand rejected under 35 USC §103 as being unpatentable over Sampson in view of US Pub 2003/0074580 to Knouse.

Claim 3 depends from Claim 1. For at least the same reasons Claim 1 is patentable, so is Claim 3.

Claim 11 depends from Claim 9. For at least the same reasons Claim 9 is patentable, so is Claim 11.

Grounds For Rejection D – Claims 4 and 12 stand rejected under 35 USC §103 as being unpatentable over Sampson in view of Knouse and in further view of USPN 2004/0015580 to Lu.

Claim 4 depends from Claim 1. For at least the same reasons Claim 1 is patentable, so is Claim 4.

Claim 12 depends from Claim 9. For at least the same reasons Claim 9 is patentable, so is Claim 12.

Grounds For Rejection E – Claims 6 and 14 stand rejected under 35 USC §103 as being unpatentable over Knouse and in further view of Lu.

Claim 6 is directed to a method, in a computer network, for locating a resource and recites the following acts:

1. providing a web page having instructions to request a web bug;
2. requesting the web bug sending a cookie and an URL for the web page;

3. saving the cookie and the URL for the web page as an entry in an association table;
4. querying, providing the URL for the web page, the association table for the cookie in the entry containing the URL;
5. identifying other entries in the association table containing the cookie;
6. identifying from those entries an entry containing an URL for an identification service, the identification service managing resource data; and
7. locating the resource using the resource data.

The Examiner asserts that Knouse, paragraph [0204] teaches the acts of saving the cookie and the URL for the web page as an entry in an association table and querying, providing the URL for the web page, the association table for the cookie in the entry containing the URL identifying an identity service using the association data. That paragraph is reproduced below to illustrate the Examiner's mistake.

> [0204] As a result, the user is transparently authenticated in both the original associated portal's domain and the e-business host's domain. The process is transparently performed for each different associated portal that a user may visit during a session. The present invention's associated portal support easily supports single Web Servers having multiple DNS names in multiple domains, and/or multiple network addresses. In accordance with the present invention, this multiple domain authentication enables "staging" of web sites. For example, a new edition of a web site can be deployed on a separate set of servers, and then mapped to policy domains protected by the present invention by simply updating the policy domain's host ID's.

Knouse, paragraph [0204].

The passage clearly mentions NOTHING of saving a cookie and an URL in an association table or providing the URL for the web page to query the association table for the cookie in the entry containing the URL.

The Examiner asserts that Knouse, paragraph. [0209] teaches the act of identifying other entries in the association table containing the cookie. That paragraph is reproduced below to illustrate the Examiner's mistake.

> [0209] Referring back to FIG. 28, if authentication event handler 512 determines that the domain of the requested resource is a master domain (step 1032), then authentication event handler 512 attempts to authenticate at the master domain (step 1034). Otherwise, redirection event handler 504 redirects browser 12 to the master domain (step 1036). The user then authenticates at the master domain (step 1038). The redirection and authentication of steps 1036 and 1038 are illustrated in FIG. 29 by path 1086. Upon a successful authentication at the master domain, the master domain Web Server passes an authentication cookie to the user's browser (step 1040) and re-directs the user's browser back to the first domain accessed by the user (step 1042). Also in step 1042, the master domain passes information contained in the master domain authentication cookie to the first domain in the query data portion of the redirection URL. Steps 1040 and 1042 are illustrated by paths 1088 and 1090, respectively in FIG. 29. In step 1044, the Web Gate of the first domain Web Server extracts the master domain authentication cookie information from the redirection URL, thus confirming the user's authentication at the master domain and resulting in a successful authentication (step 1046). The first domain Web Server (B.com) then sends its own authentication cookie to web browser 1082 (as depicted by path 1092) in accordance with step 780 of FIG. 22, previously described above. Any subsequent authentication by browser 1082 at domain C.com on Web Server 1074 follows the method of FIG. 28.

Knouse, paragraph [0209]. This cited paragraph mentions NOTHING of identifying other entries in the association table containing the cookie. The paragraph simply discusses authenticating a user at a master domain and then redirecting the user's browser to a different domain using a redirection URL that includes an authentication cookie. A server on the different domain extracts the authentication cookie from the redirection URL to confirm the user's authentication on the master domain.

The Examiner asserts that Knouse, parapraphs. [0206]-[0209] teach the act of identifying from those entries an entry containing an URL for an identification service,

the identification service managing resource data. Those paragraphs are reproduced below to illustrate the Examiner's mistake.

> [0206] If multiple domains are protected, the method proceeds to step 1024 where authentication event handler 512 determines whether the multiple protected domains all reside on a single Web Server. For example, a single machine intranet.oblix.com may be addressed in multiple ways such as: sifl.oblix.com, intranet, asterix.oblix.com, or 192.168.70.1. In accordance with the present invention, when multiple domains reside on a single Web Server, an administrator will designate exactly one of the domains a "preferred host domain." If step 1024 indicates that all protected domains reside on the same Web Server, then authentication event handler 512 determines whether the domain of the requested resource is a preferred host (step 1026). If it is a preferred host, then authentication event handler 512 attempts to authenticate the user at the preferred host domain in step 1030 (further described below with respect to FIG. 30). Otherwise, redirection event handler 504 redirects browser 12 to the preferred host domain (step 1028) for authentication (step 1030). Referring to step 1024, if the multiple protected domains reside on multiple Web Servers, then authentication event handler 512 proceeds to step 1032.
>
> [0207] In one embodiment, a single policy domain and/or policies are created for the preferred host domain while no policy domains or policies are created for the other domains residing on the same web server. All resource requests made to any of the multiple protected domains residing on the same web server are redirected to the preferred host domain, thus requiring the user to authenticate according to the preferred host domain's policy domain and/or policies. As a result, after authentication at the preferred host domain, the user is transparently authenticated for all other domains residing on the same web server. When subsequent resource requests for resources in domains residing on the same web server are redirected to the preferred host domain, the prior successful authentication for the host domain can be confirmed by the existence of a valid authentication cookie for the preferred host domain. If such a cookie exists, then the user need not re-authenticate for the requested resource. In one embodiment, if subsequent resource requests made to the preferred host domain (or any of the other domains on the same web server) require a higher level of authentication, or if a previously valid authentication has expired, the user will be required to re-authenticate at the preferred host domain in accordance with the method of FIG. 28.
>
> [0208] FIG. 29 provides a block diagram of a plurality of Web Servers, each hosting a different domain accessible by browser 1082. In

accordance with the present invention, when multiple domains are protected and distributed across multiple Web Servers, the administrator will identify exactly one of the domains a "master domain." As identified in FIG. 29, Web Server 1070 hosts master domain A.com, while Web Servers 1072 and 1074 host domains B.com and C.com, respectfully. An end user's resource request is illustrated in FIG. 29 by path 1084 from browser 1082 to Web Server 1072.

[0209] Referring back to FIG. 28, if authentication event handler 512 determines that the domain of the requested resource is a master domain (step 1032), then authentication event handler 512 attempts to authenticate at the master domain (step 1034). Otherwise, redirection event handler 504 redirects browser 12 to the master domain (step 1036). The user then authenticates at the master domain (step 1038). The redirection and authentication of steps 1036 and 1038 are illustrated in FIG. 29 by path 1086. Upon a successful authentication at the master domain, the master domain Web Server passes an authentication cookie to the user's browser (step 1040) and re-directs the user's browser back to the first domain accessed by the user (step 1042). Also in step 1042, the master domain passes information contained in the master domain authentication cookie to the first domain in the query data portion of the redirection URL. Steps 1040 and 1042 are illustrated by paths 1088 and 1090, respectively in FIG. 29. In step 1044, the Web Gate of the first domain Web Server extracts the master domain authentication cookie information from the redirection URL, thus confirming the user's authentication at the master domain and resulting in a successful authentication (step 1046). The first domain Web Server (B.com) then sends its own authentication cookie to web browser 1082 (as depicted by path 1092) in accordance with step 780 of FIG. 22, previously described above. Any subsequent authentication by browser 1082 at domain C.com on Web Server 1074 follows the method of FIG. 28.

Knouse, paragraphs. [0128]-[0129].

These paragraphs mention NOTHING of identifying from those entries an entry containing an URL for an identification service, the identification service managing resource data.

Lu fails to address Knouse's deficiencies noted above. For at least these reasons, Claim 6 is patentable over Knouse and Lu.

Claim 14 is direct to is directed to a computer readable medium having instructions for implementing the method of Claim 6. For at least the same reasons Claim 6 is patentable, so is Claim 14.

Grounds For Rejection F – Claims 7 and 15 stand rejected under 35 USC §103 as being unpatentable over Sampson in further view of Lu.

Claim 7 is directed to a method for producing an electronic document and recites the following acts:

1. generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options;
2. querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page;
3. obtaining the user's resource data from the identified identity service;
4. locating and accessing a document management service using the resource data;
5. providing additional content for the web page for displaying controls for selecting a document managed by the document management service; and
6. producing a document according to selections made through the web page.

The Examiner asserts that the act of querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page is taught by Sampson, col. 7, lines 16-20 and col. 7, line 64 through col. 8, line 5. Those passages is reproduced as follows:

> If the login attempt is successful, the system 2 presents the User with a Personalized Menu that assists the User in identifying and selecting a Resource. In one embodiment, a Personalized Menu is an HTML page containing a list of authorized Resources. The Personalized Menu displays

only Resources to which the User has access. The User can then select and access a Resource.

Sampson, col. 7, lines 16-22.

When the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server. A Protected Web Server is a web server with resources protected by the Runtime Module. The Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource. The cookie is also used by the resource to return information that is customized based on the user's name and roles.

Sampson, col. 7, line 64 through col. 8, line 5.

The first passage describes presenting a user with a personalized menu in the form of an HTML page that contains a list of authorized resources. According to the second passage, when the user selects a resource from that HTML page, a cookie is sent to a web server that is protected by a run time module. The run time module decrypts the cookie to ensure that the user is authorized to access the resource.

Nothing in this passages teaches, suggests or even hints at a method that includes querying an association service to identify an identity service with which the user is registered by providing an URL for a generated web page as recited by Claim 7. More particularly, the passage is completely unrelated to "querying the association service to identify an identity service or any other service for that matter.

Lu is silent on this point

For at least these reasons, Claim 7 is patentable over Sampson and Lu as is Claim 8 which depends from Claim 7

Claim 15 is directed to a computer readable medium having instructions for implementing the method of Claim 7. For at least the same reasons Claim 7 is patentable, so are Claim 15 and Claim 16 which depends from Claim 15.

Conclusion: In view of the foregoing remarks, the Applicant respectfully submits that the pending claims are in condition for allowance. Consequently, early and favorable action allowing these claims and passing the application to issue is earnestly solicited.

Respectfully submitted,
Gregory Eugene Perkins, et al.

By /Jack H. McKinney/
Jack H. McKinney
Reg. No. 45,685

November 1, 2007

APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

1. (original) In a computer network, a method for locating a resource, comprising:

providing an interface having instructions to send association data;

identifying an identity service using the association data, the identity service managing resource data; and

locating the resource using the resource data.

2. (original) The method of Claim 1, further comprising performing a specified task utilizing the resource.

3. (original) The method of Claim 1, wherein the association data includes a client identifier and a session identifier associated with the interface, and wherein the act of identifying comprises:

providing the session identifier associated with the interface, identifying the client identifier included in the association data;

identifying other association data containing that client identifier; and

acquiring at least a portion of the session identifier included in the other association data.

4. (original) The method of Claim 1, wherein the act of providing comprises providing a web page having instructions to request a web bug sending association data containing a cookie and an URL for the web page; and

wherein the act of identifying comprises:

providing the URL to identify the association data containing the cookie;

identifying other association data containing the cookie; and

acquiring an URL for the identity service from the identified association data.

5. (original) In a computer network, a method for locating a resource for a user,

comprising:

providing an interface having instructions to send association data to two or more association services;

identifying from the two or more association services, an association service with which the user has established a relationship;

identifying an identity service using the association data sent to the identified association service, the identity service managing resource data; and

locating the resource using the resource data.

6. (original) In a computer network, a method for locating a resource comprising:

providing a web page having instructions to request a web bug;

requesting the web bug sending a cookie and an URL for the web page;

saving the cookie and the URL for the web page as an entry in an association table;

querying, providing the URL for the web page, the association table for the cookie in the entry containing the URL;

identifying other entries in the association table containing the cookie;

identifying from those entries an entry containing an URL for an identification service, the identification service managing resource data; and

locating the resource using the resource data.

7. (original) A method for producing an electronic document, comprising:

generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options;

querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page;

obtaining the user's resource data from the identified identity service;

locating and accessing a document management service using the resource data;

providing additional content for the web page for displaying controls for selecting a document managed by the document management service; and

producing a document according to selections made through the web page.

8. (original) The method of Claim 7, wherein:

the act of generating comprises generating a web page having instructions to request a web bug sending, to the association service association, data containing a cookie and an URL for the web page;

the method further comprises saving the association data as an entry in an association table;

the act of querying further comprises identifying the cookie in the saved entry using the provided the URL, identifying other association data containing the identified cookie, and, from the other identified association data, acquiring an URL for the identity service; and

the act of obtaining the user's resource data comprises obtaining the user's resource data from the identified identity service using, at least in part, the acquired URL.

9. (original) A computer readable medium having instructions for:

providing an interface having instructions to send association data;

identifying an identity service using the association data, the identity service managing resource data; and

locating a resource using the resource data.

10. (original) The medium of Claim 9, having further instructions for performing a specified task utilizing the resource.

11. (original) The medium of Claim 9, wherein the association data includes a client identifier and a session identifier associated with the interface, and wherein the instructions for identifying comprise instructions for:

providing the session identifier associated with the interface, identifying the client identifier included in the association data;

identifying other association data containing that client identifier; and

acquiring the session identifier included in the other association data.

12. (original) The medium of Claim 9, wherein the instructions for providing comprise instructions for providing a web page having instructions to request a web bug sending association data containing a cookie and an URL for the web page; and

wherein the instructions for identifying comprise instructions for:

providing the URL to identify the association data containing the cookie;

identifying other association data containing the cookie; and

acquiring, from the identified association data, an URL for the identity service.

13. (original) A computer readable medium having instructions for:

providing an interface having instructions to send association data to two or more association services;

identifying from the two or more association services, an association service with which a user has established a relationship;

identifying an identity service using the association data sent to the identified association service, the identity service managing resource data; and

locating a resource for the user using the resource data.

14. (original) A computer readable medium having instructions for:

providing a web page having instructions to request a web bug;

requesting the web bug sending a cookie and an URL for the web page;

saving the cookie and the URL for the web page as an entry in an association table;

querying, providing the URL for the web page, the association table for the

cookie in the entry containing the URL;

identifying another entries in the association table containing the cookie;

identifying, from those entries, the entry containing an URL for an identification service, the identification service managing resource data; and

locating a resource using the resource data.

15. (original) A computer readable medium having instructions for:

generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options;

querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page;

obtaining the user's resource data from the identified identity service;

locating and accessing a document management service using the resource data;

providing additional content for the web page for displaying controls for selecting a document managed by the document management service; and

producing a document according to selections made through the web page.

16. (original) The medium of Claim 15, wherein:

the instructions for generating comprise instructions for generating a web page having instructions to request a web bug sending to the association service association data containing a cookie and an URL for the web page;

the medium having further instructions for saving the association data as an entry in an association table;

the instructions for querying further comprise instructions for identifying the cookie in the saved entry using the provided the URL, identifying other association data containing the identified cookie, and, from the other identified association data, acquiring an URL for the identity service; and

the instructions for obtaining the user's resource data comprise instructions for

obtaining the user's resource data from the identified identity service using, at least in part, the acquired URL.

17. (original) A system for locating a resource, comprising:

an association module operable to query an association service, supplying a session identifier, in order to identify an identity service managing resource data; and

an application operable to:

provide an interface having instructions to send association data to the association service, the association data to contain a client identifier and a session identifier for the provided interface;

acquire resource data from an identity service identified by a query from the association module; and

locate the resource using the resource data.

18. (original) The system of Claim 17, wherein:

the application is further operable to provide the interface in the form of a web page having instructions to send association data containing a cookie and the URL for the provided web page; and

the association module is further operable to provide the URL and query the association service for an URL for the identity service.

19. (original) A document production system, comprising:

an association module operable to query an association service, supplying a session identifier in order to identify an identity service managing resource data; and

a document production application operable to:

provide an interface having content for sending association data containing a session identifier for the provided interface to an association service as well as content for displaying controls for selecting production options;

acquire resource data from an identity service identifier identified by

a query from the association module;

locate and access a document management service using the resource data; and

provide, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and

produce a document according to selections made through the interface.

20. (original) A system for locating a resource, comprising:

an identity service operable to manage resource data;

an association server operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table;

an association table interface in communication with the association server and operable, according to a received query, to access from the association table a session identifier for the identity service using a session identifier supplied with the query;

an association module operable to query, supplying a session identifier, the association service in order to identify the identity service;

an application operable to:

provide an interface having instructions to send association data to an association server, the association data to contain a client identifier and a session identifier for the provided interface;

acquire resource data from the identity service identified by a query from the association module; and

locate the resource using the resource data.

21. (original) The system of Claim 20, wherein:

the application is further operable to provide the interface in the form of a web page having instructions to send association data containing a cookie and the URL for

the provided web page;

the association module is further operable to provide the URL interface and query the association service for an URL for the identity service; and

the association table interface is further operable to locate an entry in the association table containing the provided URL, identify the cookie in the located entry, identify other entries containing that cookie, and, from those other entries, acquire an URL for the identity service; and

the application is further operable to use the acquired URL to acquire resource data from the identity service.

22. (original) A document production system, comprising:

a document management service;

an identity service operable to manage resource data for locating and accessing the document management service;

an association server operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table;

an association table interface in communication with the association server and operable, according to a received query, to access from the association table a session identifier for the identity service using the session identifier supplied with the query;

an association module operable to query, supplying a session identifier, the association service in order to identify the identity service;

a document production application operable to:

provide an interface having content for sending association data containing a client identifier and a session identifier for the provided interface to an association service as well as content for displaying controls for selecting production options;

acquire resource data from an identity service using the session identifier for the identity service identified by a query from the association

module;

locate and access the document management service using the resource data;

provide, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and

produce a document according to selections made through the interface.

23. (original) The system of Claim 22, wherein:

the association table interface is further operable to locate an entry in the association table containing the session identifier supplied with a query, identify the client identifier in the located entry, identify other entries containing that client identifier, and, from those other entries, acquire a session identifier for the Identity service; and

the document production application is further operable to use the acquired session identifier for the identity service to acquire resource data from the identity service.

24. (original) A system for locating a resource, comprising:

a means for querying, supplying a session identifier, an association service in order to identify an identity service managing resource data;

a means for providing an interface having instructions to send association data to the association service, the association data to contain a client identifier and a session identifier for the provided interface;

a means for acquiring resource data from an identity service identified by a query; and

a means for locating the resource using the resource data.

25. (original) A document production system, comprising:

a means for querying, supplying a session identifier, an association service in

order to identify an identity service managing resource data;

a means for providing an interface having content for sending association data containing a session identifier for the provided interface to the association service as well as content for displaying controls for selecting production options;

a means for acquiring resource data from an identity service identifier identified by a query;

a means for locating and accessing a document management service using the resource data;

a means for providing, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and

a means for producing a document according to selections made through the interface.

Evidence Appendix

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix

There are no related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.